

CLAIMS

1. A computer-implemented method for management of service keys for a consortium blockchain network within a blockchain-as-a-service, BaaS, platform, the method comprising, for each of a first participant and a second participant:

at the BaaS platform:

receiving (404) an encrypted identity certificate from the participant, the identity certificate comprising a public key wherein, the BaaS platform decrypts the identity certificate using a public key of the participant;

receiving a request (408) for a service key from the participant in the consortium blockchain network provisioned within the BaaS platform;

determining (410) that the participant is authorized for the service key based on a service authorization table that records participant privileges within the consortium blockchain network;

generating the service key;

encrypting a private key of the service key using the public key comprised within the identity certificate of the participant;

providing (416) a key package comprising the encrypted private key of the service key, and a public key of the service key, wherein neither the public nor the private key of the service key is stored on the BaaS platform; and

sending (418) the key package to the participant; and

at the participant:

receiving the key package; and

decrypting the private key of the service key using a private key associated with the identity certificate of the participant; wherein,

the service key of the first participant and the service key of the second participant are public-private key pairs that enable private transactions to be conducted between the first participant and the second participant within the consortium blockchain network.

2. The method of claim 1, wherein the service key is generated using a key derivation function, KDF, key tree in response to determining that the participant is authorized for the service key.

3. A system, for management of service keys for a consortium blockchain network within a blockchain-as-a-service, BaaS, platform, the system comprising:

- one or more computers;

- one or more computer-readable memories coupled to the one or more computers and configured with instructions, which when executed by the one or more computers, for each of a first participant and a second participant;

- receive (404) an encrypted identity certificate from the participant, the identity certificate comprising a public key, wherein the BaaS platform decrypts the identity certificate using a public key of the participant;

- receive a request (408) for a service key from a participant in the consortium blockchain network provisioned within the BaaS platform;

- determine (410) that the participant is authorized for the service key based on a service authorization table that records participant privileges within the consortium blockchain network;

- generate the service key;

- encrypt a private key of the service key using the public key comprised within the identity certificate of the participant;

- provide (416) a key package comprising the encrypted private key of the service key, and a public key of the service key, wherein neither the public nor private key of the service key is stored on the BaaS platform;

- send (418) the key package to the participant, and;

- one or more further computers;

- one or more further computer-readable memories coupled to the one or more further computers and configured with instructions, which when executed by the one or more further computers:

- receive the key package;

- decrypt the private key of the service key using a private key associated with the identity certificate of the participant; wherein,

- the service key of the first participant and the service key of the second participant are public-private key pairs that enable private transactions to be conducted between the first participant and the second participant within the consortium blockchain network.